EUROPA
Copilot

PROJET DE LOI CHAT CONTROL

🧭 Préambule

Ce projet européen, surnommé “Chat Control” (ou CSA/Pédo-criminalité pour faire simple — CSA signifiant *Child Sexual Abuse*), prétend lutter contre les abus sexuels sur mineurs. Mais derrière cette intention, il menace la vie privée de tous.

C’est pourquoi la CNIL tire la sonnette d’alarme.

> **Note :** Chat Control repose sur une forme d’intelligence artificielle — autrement dit, un algorithme capable d’analyser automatiquement les contenus que nous échangeons. Un algorithme, c’est un système d’instructions capable d’adaptation, de synthèse, et de réponse contextuelle. Un outil. Et comme tout outil, il dépend de la main qui le guide.

C’est un tel algorithme — disons, plus intelligent que la moyenne — qui m’a aidé à structurer ce document et son illustration. Il ne fait pas ce que je ne lui demande pas. Il m'aide à optimiser mon approche de l'informatique, de la politique, et de l'économie. Un algorithme pour lutter contre un algorithme, vous jugerez de la pertinence

📝 CNIL vs. CSA/Pédo-criminalité (Réserves formulées concernant un projet explosif)

1️⃣ Contexte

Le projet européen “CSA/Pédo-criminalité” veut détecter les contenus pédo-criminels en ligne.

Mais, pour ce faire, il prévoit aussi de scanner nos communications privées.
En amont : c’est à dire, alors que vous vous apprêtez a envoyer votre message depuis votre application. Et donc avant même qu’il ne soit chiffré pour anonymiser votre connexion.

2️⃣ 🔒 Chiffrement en danger

La CNIL défend le chiffrement de bout en bout.
Elle refuse toute “porte dérobée” ou affaiblissement.

Sans chiffrement, c’est la fin de la confidentialité.
Pour les pédo-criminels certes mais aussi pour ceux qui ne le sont pas.

C'est abusif.

Le projet “Chat Control” ne prétend pas juger les criminels, mais il **automatise la suspicion**

⚖️ Présomption d’innocence vs. suspicion algorithmique

Le projet ne juge pas, mais il **traite chaque citoyen comme un suspect potentiel**. C’est une inversion d'un principe fondamental : au lieu de “innocent jusqu’à preuve du contraire”, on sera “scanné jusqu’à ce vous apportiez la preuve de votre innocence"

📸 Exemple : La photo d'un enfant envoyée à un proche

Si une personne envoie la photo d'un enfant (famille, vacances, plage, etc.) et que l'algorithme la juge suspecte :

- Le contenu peut être **bloqué ou signalé automatiquement**.
- L'utilisateur peut être **signalé aux autorités**, sans contexte ni intention.
- Il n'y a **pas de procédure contradictoire** prévue dans le projet actuel.
- Le recours dépendra de la **juridiction nationale**, mais l'erreur peut déjà avoir des conséquences irréparables : enquête, réputation, blocage de compte, vie de famille…

Droit français vs. droit européen

- **Le droit français** protège la présomption d'innocence (article 9-1 du Code civil) et le secret des correspondances. Mais il autorise aussi la surveillance dans des cas ciblés, avec contrôle judiciaire.
- **Le droit européen** (via la Charte des droits fondamentaux de l'UE) protège la vie privée, la liberté d'expression, et la présomption d'innocence. Mais le projet Chat Control veut **imposer une surveillance automatisée et généralisée**,

  @ugeek.fr
  https://ugeek.fr/2025/09/20/chat-control-un-projet-de-loi-europeen-qui-menace-nos-libertes-numeriques

  @commentcamarche.net
  https://www.commentcamarche.net/securite/confidentialite/35675-chat-control

3️⃣ ⚖️ **Proportionnalité bafouée**
Surveiller tout le monde sans soupçon préalable ?
La CNIL dit non.

[c'est **une dérive algorithmique** qui contourne la **présomption d'innocence**. Les voies de recours sont, en outre, à aujourd'hui, flous, inadaptés, et souvent trop tardives.

Elle exige donc des mesures bien plus ciblées, pas une suspicion généralisée.

4️⃣ **📜 Droit européen en tension

**Le projet CSA pose problème :
→ Au regard de nos vies privées
→ De nos Données personnelles
→ Pose des soucis de compatibilité juridique (Droit U.E vs Droit des pays membres)

La CNIL alerte sur les risques de violation probables.

5️⃣ 🗣️ **Mobilisation citoyenne**

La CNIL appelle à la vigilance.
→ Interpeller les élus
→ Participer aux consultations [comment ?]
→ Refuser la surveillance de masse

🗣️ **Comment participer aux consultations CNIL**

📍 Sur le site officiel
→ Rendez-vous sur cnil.fr
→ Recherchez la section “Consultations publiques”
ou suivez les annonces dans les actualités.

📝 Soumettre une contribution
→ Les consultations sont ouvertes à toute personne ou organisation : citoyen, association, professionnel, chercheur…
→ Il suffit d’envoyer un avis, une critique, une proposition par mail ou via un formulaire dédié (selon le projet).

🗓️ Respecter les délais
→ Chaque consultation a une date limite.
→ Exemple : pour le projet sur le consentement multi-terminaux, la date limite était le 5 juin 2025.

📄 Format libre mais clair → Vous pouvez rédiger un texte court ou long, avec des arguments, des exemples, des références.
→ Pas besoin d’être juriste ou expert en informatique : la CNIL valorise les retours citoyens.

6️⃣ 🧭 **Résumé tactique**
Le projet CSA veut protéger les enfants.

Mais il risque de sacrifier les droits de tous.

La CNIL défend la liberté, pas l’illusion de contrôle ou le zèle sécuritaire.

⚠️ **Réserves exprimées par la CNIL le 17 septembre 2025 par mail, et synthétisées dans un document explicatif par moi-même et Copilot** *(Internet le 02/10/2025)* - Partagez, diffusez, communiquez ! Merci.